Information sharing guidance

This document provides guidance for health, social service, academic and other organisations in Oxfordshire who need to share personal information. It envisages a sharing framework which comprises:

- An overarching *Information Sharing Agreement* which commits the organisations to the lawful processing of personal information which they may share or receive.
- *Information Sharing Protocols* provide detailed information on specific datasets which organisations have agreed to share.

The document is based predominantly on the Caldicott principles (1997) and the Data Protection Act (1998), and with reference to the NHS Confidentiality Code of Conduct (2003). In addition, the Information Commissioner's Office website contains detailed advice on the application of the Data Protection Act.

Contents

1) Definitions

a) Data (see table 1 for types of information)

Data means information which:

- is being processed by means of equipment operating automatically in response to instructions given for that purpose,
- is recorded with the intention that it should be processed by means of such equipment,
- is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
- does not fall within the criteria above but forms part of an accessible record as defined by section 68, or
- is recorded information held by a public authority and does not fall within any of the criteria above

b) Purpose (see table 2 for categories of purpose for sharing information)

Personal data must only be used for the purpose(s) for which it was obtained i.e. to enable the care of patients by health and social care workers within the community.

Patient identifiable clinical information may only be shared for the benefit of that individual (or, in exceptional circumstances, an overriding public interest).

c) Processing

Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organisation, adaptation or alteration of the information or data,
- retrieval, consultation or use of the information or data,
- disclosure of the information or data by transmission, dissemination or otherwise making available,
- alignment, combination, blocking, erasure or destruction of the information or data.

d) Confidential data / information

Data or information regarding an individual which that individual would reasonably expect to be treated in confidence, i.e. kept safe and secure and not disclosed (intentionally or unintentionally) to a third party without the individual's knowledge. In practice, all personal and clinical information collected in the course of clinical care is confidential.

e) Disclosure

The act of making new or confidential information known. In practice this refers to the transfer of information to a third party or parties. Disclosures may be classified as routine, non-routine, and mandatory or statutory.

- **A routine disclosure** of personal information is one that happens as a matter of course in relation to the direct care or treatment of the individual.
- **Non-routine disclosures** may be required by law or court order (mandatory or statutory) or may include disclosures for example in response to a request from an individual or organization undertaking a service audit.

f) Designated officer

An individual identified by the organisation as responsible for overseeing information flows and for responding to data requests from partner organisations of a non-routine nature. The individual will normally be the organisation's Caldicott Guardian, Information Governance Manager, Information Protection Officer, or someone nominated for the purpose.

Table 1: Types of information	

Personal information	• **Data which relate to a living individual who can be identified:**
	  ○ from those data, or
	  ○ from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller
	  ○ and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. (The fact that an organisation holds such data implies a purpose.)

Sensitive personal information	• **Personal data consisting of information as to:**
	  ○ the racial or ethnic origin of the data subject, or
	  ○ his/her religious beliefs or other beliefs of a similar nature, or
	  ○ his/her political opinions, or
	  ○ whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), or
	  ○ his/her physical or mental health or condition, or
	  ○ his/her sexual life, or
	  ○ the commission or alleged commission by him /her of any offence, or
	  ○ any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings.

Anonymised information	• **Data or information regarding an individual from which the person-identifying attributes have been removed**. ○ Anonymisation does not remove the requirement for confidentiality
Pseudonymised information	• **Data which has undergone the technical process of replacing person identifiers in a dataset with other values (pseudonyms), from which the identities of individuals cannot be intrinsically inferred.** ○ Examples include: replacing an NHS number with another random number; replacing a name with a code; or replacing an address with a location code

Table 2: Categories of purpose for sharing information	
Information type	**Purpose**
Identifiable personal and personal sensitive data may be shared for:	• Delivering care and treatment • Monitoring and protecting public health • Risk management • Where emotional, physical or sexual abuse or neglect are suspected • Investigating complaints and notified or potential legal claims • Equipping the courts with required information
Data should be anonymised or pseudonymised for: -	• Assuring and improving the quality of care and treatment • Teaching • Managing and planning services • Auditing accounts and accounting for performance • Contracting for services • Statistical analysis and reporting

Table 3: Categories of consent	
Consent type	**Explanation**
Explicit	• The patient has given express consent that the information may be shared; **or** • The patient has given express permission that the information may be viewed
Implicit	• The patient is aware that the information may be shared and has not objected; **or** • The patient is aware that the information may be viewed and has not objected
Note that consent of either type is only valid if given on the basis of a full understanding of the issue. Individuals must therefore be fully informed of the uses to which information collected will be put before they can give valid consent for its collection, retention, and use.	

2) The seven Caldicott principles and their interpretation

• Principle 1 - Justify the purpose(s)

Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed, by an appropriate guardian.

• Principle 2 - Don't use patient-identifiable information unless it is absolutely necessary

Patient-identifiable information items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

• Principle 3 - Use the minimum necessary patient identifiable information

Where use of patient-identifiable information is considered to be essential, the inclusion of each individual item of information should be considered and justified so that the minimum amount of identifiable information is transferred or accessible as is necessary for a given function to be carried out.

• Principle 4 - Access to patient-identifiable information should be on a strict need-to-know basis

Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to the information items that they need to see. This may mean introducing access controls or splitting information flows where one information flow is used for several purposes.

• Principle 5 - Everyone with access to patient-identifiable information should be aware of their responsibilities

Action should be taken to ensure that those handling patient-identifiable information - both clinical and non-clinical staff - are made fully aware of their responsibilities and obligations to respect patient confidentiality.

• Principle 6 - Understand and comply with the law

Every use of patient-identifiable information must be lawful. Someone in each organisation handling patient information should be responsible for ensuring that the organisation complies with legal requirements.

• Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

3) The eight principles of the Data Protection Act (1998), their interpretation and the required action for organisations

The First Principle

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless [certain] conditions are met:

At least one of the following conditions must be met for **processing personal data**:

- The individual who the personal data is about has consented to the processing
- The processing is necessary:
    - in relation to a contract which the individual has entered into;
    - or because the individual has asked for something to be done so they can enter into a contract.
- The processing is necessary because of a legal obligation that applies to you (except an obligation imposed by a contract).
- The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident.
- The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.
- The processing is in accordance with the "legitimate interests" condition.

At least one of the following conditions must be met when **processing sensitive personal data**:

- The individual who the sensitive personal data is about has given explicit consent to the processing;
- The processing is necessary so that you can comply with employment law;
- The processing is necessary to protect the vital interests of:
    - the individual (in a case where the individual's consent cannot be given or reasonably obtained);
    - or another person (in a case where the individual's consent has been unreasonably withheld);
- The processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents. Extra limitations apply to this condition;

- The individual has deliberately made the information public;
- The processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights;
- The processing is necessary for administering justice, or for exercising statutory or governmental functions;
- The processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality;
- The processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the rights of individuals.

The key components of 'fair processing' are as follows:

- how was the data obtained;
- was the data subject provided with the following information:
    - the identity of the data controller;
    - the purpose for which the data are to be processed;
    - any further information - e.g. who will have access to the data and for what purpose/s;
- was the data subject aware of all the purpose/s for which their information are to be processed, the likely consequences of such processing and whether particular disclosures can be reasonably envisaged.

Required action: each organisation must ensure they have adequate tested procedures to ensure consent for use of information is obtained.

The Second Principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

This means that information must not be used for anything other than the stated purpose. The organisation (data controller) holding the information is legally bound to notify the Information Commissioner's Office of the purpose for holding the information, details of the type of information held and to whom (organisation/agency) the information may be disclosed.

It should be noted that although it is no longer a legal requirement to notify the Information Commissioner of information sources an individual has a right to know from whom an organisation receives information about them.

> **Required action: each organisation must ensure the data protection registrations are current and updated to take account of information use/s. The organisation commits a criminal offence if it is not kept up to date and accurate.**

The Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed..

This requires that information collected must be for a justified purpose and this may need to occur on a data item by data item case.

> **Required action: each organisation must be satisfied that it can justify each data item held as part of a patient/service user record (for patient, family and staff). This will be vital if challenged by the patient/staff or as a complaint investigated by the Information Commissioner.**

The Fourth Principle

Personal data shall be accurate and, where necessary, kept up to date.

Patient/service users should be reminded of their responsibility to provide accurate information and provide information about changes to their personal circumstances e.g. name, address

> **Required action: each organisation to have tested procedures for recording information accurately and keeping information up to date (patient/service user and staff).**

The Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

Each individual organisation will take responsibility to meet its legal and policy requirements to archive information but ensure it is available to those who need it when it is needed.

The NHS must abide by the legal requirements under the Public Records Act 1958 which are defined within Records Management: NHS code of practice 2006. This applies to all records regardless of the media they may be held/retained.

Social Services have similar requirements detailed within the Social Services guidelines 'Retention of Service user Records' procedure P3.

> **Required action: each organisation to ensure information is kept for as long as required and if it needs to be kept for longer the reason MUST be justified and recorded.**

The Sixth Principle

Personal data shall be processed in accordance with the rights of data subjects under this Act. These rights are:

- right of subject access;
- right to prevent processing likely to cause harm or distress;

- right to prevent processing for the purposes of direct marketing;
- right in relation to automated decision taking;
- right to take action for compensation if the individual suffers damage;
- right to take action to rectify, block, erase or destroy inaccurate data;
- right to make a request to the Information Commissioner for an assessment to be made as to whether any provision of the Act has been contravened.

Required action: each organisation must ensure they have up to date procedures to deal with patient/service user and staff requests for access to information held about them and for dealing with complaints for breach of above.

The Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Compliance with BS7799 Standard for Information Management and Security

The Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

4) Other relevant legislation

a) Human Rights Act 2000

This Act became law on 2 October 2000. It binds public authorities including Health Authorities, Trusts, Primary Care Groups and individual doctors treating NHS patients to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a patient/service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that '*everyone has the right to respect for his private and family life, his home and his correspondence*'. However, this article also states '*there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*'.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

b) Freedom of Information Act 2000

This Act came into force in November 2000. The Information Commissioner (previously the Data Protection Commissioner) oversees the implementation of this Act. This Act gives individuals rights of access to information held by public authorities, but not to personal identifiable data.

c) Regulation of Investigatory Powers Act 2000

This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation in this area in the light of the Human Rights laws and rapidly changing technology.

d) Crime and Disorder Act 1998

This Act allows disclosures of information (including that which identifies a person) to the Police, Local Authorities, Probation Service or Health Service where disclosure is necessary or expedient for the purposes of any provision of the Act.

The provisions of the Act include Orders (e.g. Anti-Social Behaviour and Sex Offender Orders) and the formulation and implementation of local Crime and Disorder Strategies. Furthermore the Act imposes a duty on Health Authorities (and other authorities) to exercise their various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent, crime and disorder in the area.

The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. To allow information sharing under the Crime and Disorder Act each participating organisation must sign up to a Crime and Disorder Protocol.

e) The Computer Misuse Act 1990

This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue each EHSCR user an individual user id and password, which will only be known by the individual they relate to, and must not be divulged/misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

f) The Access to Health Records 1990

This Act gives patient/service users' representatives right of access to their manually held health records, in respect of information recorded on or after 1 November 1991. This Act is only applicable for access to deceased persons records. All other requests for access to information by living individuals are provided under the access provisions of the Data Protection Act 1998.

g) Health and Social Care Act 2001: Section 60

Section 60 of the Health and Social Care Act 2001 makes it lawful to disclose and use confidential patient information in specified circumstances where it is not currently practicable to satisfy the common law confidentiality obligations. This does not create new statutory gateways, so the processing must still be for a lawful function, but does mean that consent may not have to be obtained in certain circumstances, for example when it is in the public interest and/or when it is impracticable to do so. Section 60 was intended primarily as a temporary measure until anonymization measures or appropriate recording of consent have been put in place. Even where these powers apply however, the Data Protection Act 1998 also continues to apply.

The Health Service (Control of Patient Information) Regulations 2002 were the first regulations to be made under section 60 of this Act, and support the operations of cancer registries and the Public Health Laboratory Services in respect of communicable diseases and other risks to public health.

In order to use confidential information without consent it is necessary to seek permission from the Confidentiality Advisory Group (CAG) of the NHS Health Research Authority. Further details can be obtained from

http://www.hra.nhs.uk/research-community/applying-for-approvals/confidentiality-advisory-group-cag/

Where the powers provided by this legislation are used to support the processing of confidential patient information there will be additional safeguards and restrictions on the use and disclosure of the information. These may differ from case to case and change over time where the process of annual review required by the legislation results in more stringent safeguards being applied.

5) Obtaining consent and disclosing personal information

a) Consent to disclosure

Individuals generally have the right to object to the use and disclosure of confidential information that identifies them, and need to be made aware of this right. Sometimes, if patients choose to prohibit information being disclosed to other health professionals involved in providing care, it might mean that the care that can be provided is limited and, in extremely rare circumstances, that it is not possible to offer certain treatment options. Patients must be informed if their decisions about disclosure have implications for the provision of care or treatment. Clinicians cannot usually treat patients safely, nor provide continuity of care, without having relevant information about a patient's condition and medical history.

Explicit consent is not usually required for information disclosures needed to provide that healthcare, provided that patients have been informed of:

- the use and disclosure of their information associated with their healthcare; and
- the choices that they have and the implications of choosing to limit how information may be used or shared

Even so, opportunities to check that patients understand what may happen and are content should be taken. Special attention should be paid to the issues around child consent.

Where the purpose is not directly concerned with the healthcare of a patient however, it would be wrong to assume consent. Additional efforts to gain consent are required or alternative approaches that do not rely on identifiable information will need to be developed.

There are situations where consent cannot be obtained for the use or disclosure of patient identifiable information, yet the public good of this use outweighs issues of privacy. Section 60 of the Health and Social Care Act 2001 currently provides an interim power to ensure that patient identifiable information, needed to support a range of important work such as clinical audit, record validation and research, can be used without the consent of patients.

b) Obtaining consent

Consent will be sought from the patient/service user at the first contact, in any of the participating organisations. Their record will then be flagged with their wish. The patient/service user will be made aware at this time that if he/she gives their consent all healthcare professionals involved in their treatment would have access to their information or a subset of it **(partial consent)** during the life of the care process.

Should the patient/service user wish to withdraw consent this can be done at any time by contacting a designated central contact point, that is, either the Caldicott Guardian or Data Protection Officer of one of the partner organisations, the patient/service user consent flag will be removed, and all Partner Organisations notified.

The patient/service user will be given an information leaflet explaining: how their information will be used; who will have access to their information and why; how they can withdraw consent it they wish, and an explanation of the role of the Caldicott Guardian

If the patient/service user does not consent to having personal information shared electronically then it should be explained that their treatment will be dealt with in a normal manner.

c) Recording Consent

Organisations must have a means by which an patient /service user or their guardian can record whether they give consent to the disclosure of personal information and what limits, if any, they wish placed on that disclosure.

These limitations should be overridden only if there are statutory grounds for doing so and one of the conditions of Schedule 2 of the Data Protection Act 1998 can be demonstrated. For sensitive information, one of the conditions of Schedule 3 of the Data Protection Act 1998 must also exist.

Patients/service users should be able to prescribe, in respect of all information held by the contact organisation:

- Which organisations information can and cannot be shared with
- What information known to the contact organisation can be shared and what information should remain confidential.

In addition, in respect of sensitive information (as defined by the Data Protection Act 1998) which is held by the contact organisation, the patient/service user must be able to prescribe the explicit purposes for which they agree to this information being disclosed to another organisation.

The patient/service user must have access to their files in order to comprehend what information an organisation holds about them and must be given an opportunity to amend and correct any information which is incorrect.

It is recognised that, in an urgent or emergency situation and in many routine referrals, it is impractical for existing patient/service user records to be studied in detail and amended at that point in time. All organisations should therefore have procedures in place to ensure that patient/service users are fully informed at all times of the content of their records (both manual and computerised) and have opportunities to amend the contents if they are wrong.

Under no circumstances will consent be sought, or taken to have been given, unless the individual or their representative has been fully informed of the consequences of giving consent.

If a patient/service user limits the disclosure of information in any way, then this must be flagged on their records in such a manner that any member of staff subsequently involved with that person, is alerted to this limitation of consent. Information which is held with this limitation should be stored in such a manner that access can be controlled. This limitation of consent should be recorded whether or not a decision is taken to disclose without consent.

Consent to disclosure of personal information for a particular purpose, will be limited to a period *to be specified within individual protocols*, unless the individual concerned withdraws consent in the interim period. A record must be kept of the date on which consent was given, the date on which it is due to expire and the date on which it was withdrawn, if applicable. If at any time following the withdrawal or expiry of consent, an organisation wishes to disclose that information for the same or another purpose, then consent will need to be sought again.

d) Disclosing Information without Consent

Passing information without consent places both individual staff members and organisations at risk of prosecution. If there is no lawful basis for disclosing information without consent, there is also the risk of a compensation order under the Data Protection Act, or damages for breach of confidence/breach of the Human Rights Act - Article 8 rights.

The disclosure of personal information without consent must be justifiable on statutory grounds and meet one of the conditions of Schedule 2 of the Data Protection Act 1998.

In addition, the disclosure of “sensitive” information without consent must meet one of the conditions of Schedule 3 of the Data Protection Act 1998.

If information is disclosed without consent, then full details must be recorded about the information disclosed, the reasons why the decision to disclose was taken, the person who authorised the disclosure and the person(s) to whom it was disclosed. Individual protocols will specify the person(s) responsible for ensuring this happens.

A record of the disclosure will be made in the patient/service user's case file and the patient/service user must be informed if they have the capacity to understand.

Additional reference material

General Medical Council Ethical Guidance: Confidentiality

Information Commissioner s Office: Data Protection

British Medical Association: Confidentiality Toolkit

Department of Health: Caldicott Guardian Manual 2010

Department of Health: Confidentiality: NHS Code of Practice